Before the
HOUSE TELECOMMUNICATIONS SUBCOMMITTEE
Hearing on Cellular Privacy
February 5, 1997

TESTIMONY of GARY SHAPIRO
President
Consumer Electronics Manufacturers Association

SUMMARY

The Consumer Electronics Manufacturers Association, a sector of the Electronic Industries Association, represents all consumer electronics product manufacturers, including scanner and telephone makers.

Scanners are beneficial products whose usage and design has been regulated to meet privacy concerns. The present law appears flexible enough to allow the FCC to plug technical holes as they develop. There is one hole in the law which Congress should consider plugging: a side industry has developed which modifies scanners to receive cellular phone calls. Congress should consider making this practice illegal.

Cellular telephones are enormously popular with market penetration of 34 percent. CEMA projects nine million cellular telephones will be sold in 1997 (a 25 percent jump over 1996). Increasingly, consumers are buying digital telephones which are less likely to be intercepted and deciphered.

However, there is a lower expectation of privacy with cellular telephones. Most cellular consumers believe cellular calls are less secure than corded or cordless phones and appear unconcerned about this. Indeed, relatively few cellular customers would pay a 20 percent premium to receive a 100 percent secure call.

The bottom line is that both scanners and cellular telephones are popular, beneficial consumer items. Little, if any, tweaking with the law is necessary as technology improves and Americans who care about cellular privacy invest in newer technologies.

Before the
HOUSE TELECOMMUNICATIONS SUBCOMMITTEE
Hearing on Cellular Privacy
February 5, 1997

TESTIMONY of GARY SHAPIRO
President
Consumer Electronics Manufacturers Association

INTRODUCTION

My name is Gary Shapiro. I am President of the Consumer Electronics Manufacturers Association (CEMA) a sector of the Electronic Industries Association (EIA). Thank you for inviting me today to present the views of the radio scanner and cellular telephone manufacturers regarding cellular telephone privacy issues.

EIA includes in its membership all the leading manufacturers of electronics products. CEMA represents manufacturers of communications products including telephones, home entertainment products such as televisions, stereos, and video recorders, and home information equipment such as personal computers and multimedia devices, as well as many other consumer electronics products. Our members represent roughly 250,000 U.S. manufacturing jobs and about $64 billion in annual sales.

As the trade association for the consumer electronics industry, our membership includes both manufacturers of cellular telephones and radio scanning devices. Thus, CEMA is critically interested in helping find answers to the problems before us today.

My testimony can be summarized as follows:

Scanners are popular products that contribute to public safety and communication. Scanner manufacturers recognize privacy concerns and are moving to try to stay ahead of those who make a business out of illegal interception of phone calls.

The challenge we face is that no telephone conversation can ever be 100 percent secure. Most consumers understand this, especially for cellular conversations. Fortunately, technological advances, especially digital technology, will soon provide Americans added security and privacy.

I. Scanners Are Popular And Useful

A scanner is simply an information radio that allows the listener to monitor public communications such as those of police, fire departments, emergency and other services.

The four companies which make and sell scanners (AOR, ICOM, Tandy and Uniden) together sell several hundred thousand units annually. Up to ten million Americans are believed to own scanners.

Scanners are used by:

- ***Volunteer Firefighters*** -- who may hear news of an emergency prior to official notification.
- ***Police Officers*** -- to learn of potential emergencies.
- ***Wrecker Operators*** -- to learn of disabled vehicles.
- ***Journalists and Photographers*** -- to receive first notice of emergencies.
- ***Motorists*** -- who want to avoid accidents and know weather and road conditions.
- ***NASCAR Fans*** -- to monitor talk between drivers and pit crews.
- ***Consumers*** -- for entertainment and to learn of emergencies in their area.

One trade publication stated:

> "[S]canners can serve a genuinely useful function in matters of local, or even national, emergency. As one manufacturer points out, when the nuclear power plant crisis occurred at Pennsylvania's Three Mile Island, local authorities themselves bought hundreds of scanners and supplied them to people living in the vicinity in order to keep them alerted to any important news or instructions."[1]

While we are not aware of any definitive study, stories abound how scanners helped save lives:

For example, a St. Louis helicopter pilot listening on a scanner heard police describing a man holding onto a bridge above a river. Police worked with the helicopter pilot to save the man's life.[2]

II. The Law Has Adapted To Changing Technologies

Before 1986, no federal restrictions existed for scanners. In 1986, Congress passed the Electronics Communications Privacy Act which made it illegal to intercept and disclose wire, oral or electronic communications.[3] Congress at the same time also clearly indicated that it is not unlawful to access an electronic communication made through an electronic communications system that is configured to be readily accessible to the general public.

But concerns over radio scanner reception of cellular phone conversations increased as those phones became more and more popular with American consumers. In 1992, Congress

---

[1] *HFD Buyer's Guide to Scanners p.7* (May *25, 1992)*

[2] St. Louis Dispatch, p. 14 (June 14, 1991)

[3] In the Act, Congress recognized the lesser expectation of privacy for wireless telephone conversations by imposing reduced burdens on their intercept. The penalties for interception and disclosure of a wireless/wireline call is less stringent than the penalty for strictly wireline. Furthermore, the penalty for interception and disclosure of an all wireless call is less stringent still -- a monetary fine only.

authorized the FCC to deny authorization for any scanner that receives cellular frequencies or can be readily altered by the user to receive cellular frequencies or be equipped with decoders that convert digital cellular transmissions to analog voice audio.

Thus, the FCC responded by banning certain scanners as of April 1994. In particular, those rules ban the manufacturer or sale of scanners which tune or can readily be altered by the user to tune cellular telephone frequencies. The rule specifically defines "readily be altered by the user" as including the ability to receive cellular transmissions by "clipping the leads of, or installing, a simple component such as a diode, resistor and/or jumper wire," etc.

III. Scanner Manufacturers Have Stepped Up To Address Recent Concerns

One area of recent concern is the "image frequencies" generated by cellular calls.

The image frequency of a cellular call is a shadow of the original cellular signal which can sometimes be received on a scanner. The physical properties of the radiowaves and the devices that tune them present this privacy concern. Image frequencies of cellular phone conversations (in the 800 MHz band) can occur outside the cellular band as the other radio frequencies, which are being legitimately tuned, are modulated and remodulated into an audible frequency for reception through a radio speaker. These image frequencies allow legal, non-cellular band, not easily-alterable radio devices, innocently to intercept cellular telephone conversations. Compounding the problem, information about image frequencies and where they are most likely to occur has been recently disseminated in on-line services on the Internet and elsewhere.

The misuse and illicit use of image frequencies has recently come to the attention of the scanner manufacturers. To address this situation, Uniden, has asked the FCC to impose a new

solution for image frequency pickup.[4] The proposal is to have the FCC impose a minimum image rejection ratio for frequencies assigned to the cellular bands for all scanners manufactured or imported for sale in the U.S. In other words, the scanners would make image frequencies completely inaudible. In addition, the proposal suggests a new requirement that all applications for equipment authorization (i.e. certification) for scanners be accompanied by a circuit description and test data documenting compliance with the image rejection specification. The FCC has the authority to grant this request. If accepted, all new scanners after a defined date cannot, without alteration, receive images of cellular frequencies.

Some manufacturers have used filters to block the receipt of image frequencies. But, as often happens, these filters have been compromised by unscrupulous individuals. Because the aforementioned filter method has been "broken," it is necessary to employ a new way to keep this technique from being defeated.

IV. Further Congressional Action May Be Appropriate

Even with this solution there is a hole in the law. The law arguably allows anyone to offer a technique or service to adjust scanners so they can illegally receive cellular conversations. This activity is clearly aimed at facilitating illegal activity and should itself be illegal. We would likely support clarifying legislation or regulation in this area.

V. Consumers Recognize that Cellular Telephones Provide Less Security

To prepare for this hearing, on Monday and Tuesday we asked some 150 Americans who have used a cellular telephone what they thought about cellular telephone privacy.

[4] Tandy/Radio Shack supports this petition in principle but is examining the technical details.

The bottom line is that most cellular telephone users believe their conversations on cellular phones are less secure than corded phones at home.

The trade-off between security and cost indicates that most Americans with cellular telephones are willing to accept lessened privacy rather than pay a premium for a secure telephone. Fewer than one out of four American cellular telephone users would pay a 20 percent premium for a cellular telephone which is 100 percent secure.

VI. New Telephone Technologies Will Resolve Many of These Issues

Cellular telephones used to be all analog. Analog calls can be intercepted by scanners modified to receive calls in the 824-894 MHz range.

The fact is the world is going digital. A scanner can intercept a digital cellular telephone signal but cannot understand the signal.

All PCS is digital. Cellular and 900 MHz phones are increasingly digital. We estimate that 10 percent of the 7.2 million cellular phones sold in 1996 were digital. We estimate that of the nine million cellular telephones we project to be sold in 1997 -- 2 million or 22 percent will be digital.

Furthermore, the Telecommunications Industry Association (TIA), also a sector of EIA, recently set an industry standard on encryption for digital telecommunications. Digital encryption adds another level of security to all communications. We would encourage cellular service producers to consider employing this standard.

CONCLUSION

Mr. Chairman, it is clear that no telephone conversation is completely secure. Certainly no wireless communication is totally secure from a determined individual with sufficient resources. We can increase the deterrence for illicit interception and disclosure of wireless telephone conversations by clarifying current law and by strengthening technical barriers to electronic eavesdropping.

Thank you for giving me the opportunity to present these views.